The Analytic Class Number Formula

...with no proofs whatsoever

Swayam Chube
Guide: Prof. Sandeep Varma

IIT Bombay

June 21, 2024

Some Preliminaries

- A *number field K* is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial.

Some Preliminaries

- A *number field* K is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial. The algebraic integers in K form a ring, known as the *ring of integers* of K, often denoted by $\mathcal{O}_K$.

Some Preliminaries

- A *number field* K is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial. The algebraic integers in K form a ring, known as the *ring of integers* of K, often denoted by $\mathcal{O}_K$. The *group of units* in K is the multiplicative group $\mathcal{O}_K^\times \subseteq \mathcal{O}_K$.

Some Preliminaries

- A *number field* K is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial. The algebraic integers in K form a ring, known as the *ring of integers* of K, often denoted by $\mathcal{O}_K$. The *group of units* in K is the multiplicative group $\mathcal{O}_K^\times \subseteq \mathcal{O}_K$.
- A *fractional ideal* in K is an $\mathcal{O}_K$-submodule M of K such that there exists a $d \in \mathcal{O}_K$ with $dM \subseteq \mathcal{O}_K$.

Some Preliminaries

- A *number field* K is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial. The algebraic integers in K form a ring, known as the *ring of integers* of K, often denoted by $\mathcal{O}_K$. The *group of units* in K is the multiplicative group $\mathcal{O}_K^\times \subseteq \mathcal{O}_K$.
- A *fractional ideal* in K is an $\mathcal{O}_K$-submodule M of K such that there exists a $d \in \mathcal{O}_K$ with $dM \subseteq \mathcal{O}_K$. The **nonzero** fractional ideals in K form a group under multiplication (with identity element $\mathcal{O}_K$), denoted $\mathscr{I}_K$.

Some Preliminaries

- A *number field* K is a finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is said to be an *algebraic integer* if it is the root of a **monic** integer polynomial. The algebraic integers in K form a ring, known as the *ring of integers* of K, often denoted by $\mathcal{O}_K$. The *group of units* in K is the multiplicative group $\mathcal{O}_K^\times \subseteq \mathcal{O}_K$.
- A *fractional ideal* in K is an $\mathcal{O}_K$-submodule M of K such that there exists a $d \in \mathcal{O}_K$ with $dM \subseteq \mathcal{O}_K$. The **nonzero** fractional ideals in K form a group under multiplication (with identity element $\mathcal{O}_K$), denoted $\mathscr{I}_K$.
- The *class group* C_K of K is the cokernel of the natural map $K^\times \longrightarrow \mathscr{I}_K \twoheadrightarrow C_K \to 0$.

More Preliminaries

Theorem (Minkowski)

C_K is a finite group.

The cardinality h_K of C_K is known as the *class number* of K.

More Preliminaries

Theorem (Minkowski)

C_K is a finite group.

The cardinality h_K of C_K is known as the *class number* of K.

Theorem (Dedekind)

Every nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be factorized uniquely as a product of prime ideals, $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.

It follows that $\mathcal{O}_K/\mathfrak{a}$ is a finite ring and is cardinality is called the *ideal norm* of $\mathfrak{a}$, denoted $\|\mathfrak{a}\|$. One can show that $\|\mathfrak{a}\| = \prod_{i=1}^{r} \|\mathfrak{p}_i\|^{e_i}$

More Preliminaries

Theorem (Minkowski)

C_K is a finite group.

The cardinality h_K of C_K is known as the *class number* of K.

Theorem (Dedekind)

Every nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be factorized uniquely as a product of prime ideals, $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.

It follows that $\mathcal{O}_K/\mathfrak{a}$ is a finite ring and is cardinality is called the *ideal norm* of $\mathfrak{a}$, denoted $\|\mathfrak{a}\|$. One can show that $\|\mathfrak{a}\| = \prod_{i=1}^{r} \|\mathfrak{p}_i\|^{e_i}$

- If $\mathfrak{p}$ is a nonzero prime ideal in $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p and hence, $\|\mathfrak{p}\| \geq p$.

More Preliminaries

Theorem (Minkowski)

C_K is a finite group.

The cardinality h_K of C_K is known as the *class number* of K.

Theorem (Dedekind)

Every nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be factorized uniquely as a product of prime ideals, $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.

It follows that $\mathcal{O}_K/\mathfrak{a}$ is a finite ring and is cardinality is called the *ideal norm* of $\mathfrak{a}$, denoted $\|\mathfrak{a}\|$. One can show that $\|\mathfrak{a}\| = \prod_{i=1}^{r} \|\mathfrak{p}_i\|^{e_i}$

- If $\mathfrak{p}$ is a nonzero prime ideal in $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p and hence, $\|\mathfrak{p}\| \geq p$.
- Thus, for every $\lambda > 0$, there are finitely many ideals $\mathfrak{a}$ with $\|\mathfrak{a}\| \leq \lambda$. The number of such ideals is $O(\lambda)$. (See, for example, Chapter 6 of the book *Number Fields* by Daniel Marcus.)

The Dedekind Zeta Function

- Let j_n denote the number of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $\|\mathfrak{a}\| = n$. We remarked in the previous slide that $\displaystyle\sum_{m \leq n} j_m = O(n)$.

The Dedekind Zeta Function

- Let j_n denote the number of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $\|\mathfrak{a}\| = n$. We remarked in the previous slide that $\displaystyle\sum_{m \le n} j_m = O(n)$.
- The series

$$\sum_{n \ge 1} \frac{j_n}{n^s}$$

converges for $\operatorname{Re} s > 1$ and defines a holomorphic function. This is called the *Dedekind zeta function* and is denoted by $\zeta_K(s)$.

The Dedekind Zeta Function

- Let j_n denote the number of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $\|\mathfrak{a}\| = n$. We remarked in the previous slide that $\displaystyle\sum_{m \le n} j_m = O(n)$.
- The series
$$\sum_{n \ge 1} \frac{j_n}{n^s}$$
converges for $\operatorname{Re} s > 1$ and defines a holomorphic function. This is called the *Dedekind zeta function* and is denoted by $\zeta_K(s)$.
- Informally, you can think of this series as
$$\sum_{0 \ne \mathfrak{a} \trianglelefteq \mathcal{O}_K} \frac{1}{\|\mathfrak{a}\|^s}.$$
Notice that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.

The Dedekind Zeta Function

- Let j_n denote the number of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $\|\mathfrak{a}\| = n$. We remarked in the previous slide that $\sum_{m \leq n} j_m = O(n)$.
- The series

$$\sum_{n \geq 1} \frac{j_n}{n^s}$$

converges for $\operatorname{Re} s > 1$ and defines a holomorphic function. This is called the *Dedekind zeta function* and is denoted by $\zeta_K(s)$.
- Informally, you can think of this series as

$$\sum_{0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K} \frac{1}{\|\mathfrak{a}\|^s}.$$

Notice that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Like the Riemann zeta function, this too admits a *meromorphic continuation* to the entire complex plane with a simple pole at $s = 1$.

Absolute Values on Fields

- An *absolute value* on K is a map $v : K \to \mathbb{R}_{\geq 0}$ such that:
  1. $v(x) = 0$ if and only if $x = 0$.
  2. $v(xy) = v(x)v(y)$ for all $x, y \in K$.
  3. $v(x + y) \leq v(x) + v(y)$ for all $x, y \in K$.

  If further, $v(x + y) \leq \max\{v(x), v(y)\}$, then v is said to be a *non-archimedean absolute value*.

Absolute Values on Fields

- An *absolute value* on K is a map $v : K \to \mathbb{R}_{\geq 0}$ such that:
  1. $v(x) = 0$ if and only if $x = 0$.
  2. $v(xy) = v(x)v(y)$ for all $x, y \in K$.
  3. $v(x + y) \leq v(x) + v(y)$ for all $x, y \in K$.

  If further, $v(x + y) \leq \max\{v(x), v(y)\}$, then v is said to be a *non-archimedean absolute value*.
- Every absolute value induces a metric on K which can be completed and the completion K_v has a natural structure of a field such that the inclusion $K \hookrightarrow K_v$ is a field homomorphism.

Absolute Values on Fields

- An *absolute value* on K is a map $v : K \to \mathbb{R}_{\geq 0}$ such that:
  1. $v(x) = 0$ if and only if $x = 0$.
  2. $v(xy) = v(x)v(y)$ for all $x, y \in K$.
  3. $v(x + y) \leq v(x) + v(y)$ for all $x, y \in K$.

  If further, $v(x + y) \leq \max\{v(x), v(y)\}$, then v is said to be a *non-archimedean absolute value*.
- Every absolute value induces a metric on K which can be completed and the completion K_v has a natural structure of a field such that the inclusion $K \hookrightarrow K_v$ is a field homomorphism.
- The field K_v is what is known as a *local field* (owing to it being locally compact) and has its own "ring of integers"

$$\mathcal{O}_v = \{x \in K_v \colon v(x) \leq 1\} ,$$

  which is a local ring.

Ideles

- The group of ideles is the restricted direct product

$$\prod_v{}' (K_v^\times, \mathcal{O}_v^\times) = \{(x_v) \colon x_v \in \mathcal{O}_v^\times \text{ for almost all } v\},$$

and is denoted by $\mathbb{I}_K$.

Ideles

- The group of ideles is the restricted direct product

$$\prod_v{}' (K_v^\times, \mathcal{O}_v^\times) = \left\{ (x_v) \colon x_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\},$$

  and is denoted by $\mathbb{I}_K$.
- The *norm* of an idele (x_v) is defined to be

$$\prod_v v(x_v).$$

  The subgroup of norm 1 ideles is denoted by $\mathbb{I}_K^1$.

Ideles

- The group of ideles is the restricted direct product
$$\prod_v{}' (K_v^\times, \mathcal{O}_v^\times) = \left\{ (x_v) \colon x_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\},$$
and is denoted by $\mathbb{I}_K$.
- The *norm* of an idele (x_v) is defined to be
$$\prod_v v(x_v).$$
The subgroup of norm 1 ideles is denoted by $\mathbb{I}_K^1$.
- Let S be a finite set of absolute values of K and define the S-*ideles* of K to be
$$\mathbb{I}_{K,S} = \left\{ (x_v) \colon x_v \in \mathcal{O}_v^\times \text{ for all } v \notin S \right\}.$$
Their norm 1 version is denoted by $\mathbb{I}_{K,S}^1 = \mathbb{I}_{K,S} \cap \mathbb{I}_K^1$.

The Regulator

- Let $S = S_\infty$ be the Archimedean absolute values of K. Define the *logarithmic map* $\lambda : \mathbb{I}^1_{K,S_\infty} \to \mathbb{R}^{r_1+r_2}$ by

$$x = (x_v) \mapsto (\log v(x_v))_{v \in S_\infty},$$

where r_1 and r_2 are the number of real and non-conjugate complex embeddings of K into $\mathbb{C}$.

The Regulator

- Let $S = S_\infty$ be the Archimedean absolute values of K. Define the *logarithmic map* $\lambda : \mathbb{I}^1_{K,S_\infty} \to \mathbb{R}^{r_1+r_2}$ by

$$x = (x_v) \mapsto (\log v(x_v))_{v \in S_\infty},$$

  where r_1 and r_2 are the number of real and non-conjugate complex embeddings of K into $\mathbb{C}$.
- One can show that the image of the logarithm map is precisely the hyperplane H in $\mathbb{R}^{r_1+r_2}$ given by

$$\sum_{v \text{ real}} t_v + 2 \sum_{v \text{ complex}} t_v = 0.$$

The Regulator

- Let $S = S_\infty$ be the Archimedean absolute values of K. Define the *logarithmic map* $\lambda : \mathbb{I}^1_{K,S_\infty} \to \mathbb{R}^{r_1+r_2}$ by

$$x = (x_v) \mapsto (\log v(x_v))_{v \in S_\infty},$$

  where r_1 and r_2 are the number of real and non-conjugate complex embeddings of K into $\mathbb{C}$.
- One can show that the image of the logarithm map is precisely the hyperplane H in $\mathbb{R}^{r_1+r_2}$ given by

$$\sum_{v \text{ real}} t_v + 2 \sum_{v \text{ complex}} t_v = 0.$$

- The restriction of λ to $\mathcal{O}_K^\times = K^\times \cap \mathbb{I}^1_K$ is called the *regulator map* and its image is a full lattice L in H. The volume of the fundamental parallelotope H/L of this lattice is called the *regulator* and is denoted by R_K.

The Discriminant

- Since $\mathcal{O}_K$ is a finitely generated torsion free $\mathbb{Z}$-module, it must be free.

The Discriminant

- Since $\mathcal{O}_K$ is a finitely generated torsion free $\mathbb{Z}$-module, it must be free. Further, $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$ whence $\mathcal{O}_K$ has rank n.

The Discriminant

- Since $\mathcal{O}_K$ is a finitely generated torsion free $\mathbb{Z}$-module, it must be free. Further, $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$ whence $\mathcal{O}_K$ has rank n.
- We can therefore find $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \bigoplus_{j=1}^{n} \mathbb{Z}\alpha_j.$$

The Discriminant

- Since $\mathcal{O}_K$ is a finitely generated torsion free $\mathbb{Z}$-module, it must be free. Further, $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$ whence $\mathcal{O}_K$ has rank n.
- We can therefore find $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \bigoplus_{j=1}^{n} \mathbb{Z}\alpha_j.$$

- Define the *discriminant* of K to be the quantity

$$\Delta_K = \det \begin{pmatrix} \sigma_1\alpha_1 & \cdots & \sigma_1\alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \cdots & \sigma_n\alpha_n \end{pmatrix}^2 = \det \begin{pmatrix} \mathrm{Tr}(\alpha_1^2) & \cdots & \mathrm{Tr}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}(\alpha_n^2) \end{pmatrix}$$

  where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of $K \hookrightarrow \overline{\mathbb{Q}}$. Note that $\Delta_K \in \mathbb{Z}$.

The Volume of C_K^1

The cokernel of the natural map $K^\times \hookrightarrow \mathbb{I}_K^1$ is denoted by C_K^1.

The Volume of C_K^1

The cokernel of the natural map $K^\times \hookrightarrow \mathbb{I}_K^1$ is denoted by C_K^1.

Theorem (Tate)

$$\operatorname{Res}_{s=1} \zeta_K(s) = \operatorname{Vol}\left(C_K^1\right) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|\Delta_K|}}$$

where w_K is the number of roots of unity in K.

For Cyclotomic Fields

Let ζ_m denote a primitive m-th root of unity and set $F_m = \mathbb{Q}(\zeta_m)$. It can then be shown that

$$\zeta_{F_m}(s) = \zeta(s) \prod_{\substack{\chi \bmod m \\ \chi \neq 1}} L(s, \chi),$$

where the product ranges over all *Dirichlet characters* $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

For Cyclotomic Fields

Let ζ_m denote a primitive m-th root of unity and set $F_m = \mathbb{Q}(\zeta_m)$. It can then be shown that

$$\zeta_{F_m}(s) = \zeta(s) \prod_{\substack{\chi \bmod m \\ \chi \neq 1}} L(s, \chi),$$

where the product ranges over all *Dirichlet characters* $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. Since the L-series corresponding to non-trivial Dirichlet characters is holomorphic around $s = 1$ (See, for example, Chapter 6 of the book *A Course in Arithmetic* by J.P. Serre)

$$\frac{(2\pi)^{\varphi(m)/2} h_m R_m}{w_m \sqrt{|\Delta_m|}} = \prod_{\substack{\chi \bmod m \\ \chi \neq 1}} L(1, \chi)$$

Computing $L(1, \chi)$

Let χ be a Dirichlet character modulo m. Then,

$$L(1,\chi) = \begin{cases} \dfrac{g(\chi)}{m^2}\pi i \displaystyle\sum_{a=1}^{m} \overline{\chi}(a)a & \text{if } \chi(-1) = -1 \\ -\dfrac{g(\chi)}{m} \displaystyle\sum_{a=1}^{m} \overline{\chi}(a) \log\left|1 - e^{-2\pi i a/m}\right| & \text{if } \chi(-1) = 1, \end{cases}$$

where $g(\chi)$ is the *Gauss sum*

$$\sum_{a=1}^{m} \chi(a) e^{2\pi i a/m}.$$

An Application?

We shall consider the case $K = \mathbb{Q}[i] = \mathbb{Q}(\zeta_4)$. Its ring of integers is $\mathbb{Z}[i]$, which is a PID and hence, $h_K = 1$.

An Application?

We shall consider the case $K = \mathbb{Q}[i] = \mathbb{Q}(\zeta_4)$. Its ring of integers is $\mathbb{Z}[i]$, which is a PID and hence, $h_K = 1$. Now, $\{1, i\}$ forms an integral basis. A simple computation gives

$$\Delta_K = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4.$$

An Application?

We shall consider the case $K = \mathbb{Q}[i] = \mathbb{Q}(\zeta_4)$. Its ring of integers is $\mathbb{Z}[i]$, which is a PID and hence, $h_K = 1$. Now, $\{1, i\}$ forms an integral basis. A simple computation gives

$$\Delta_K = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4.$$

Finally, $r_1 = 0$ and $r_2 = 1$, whence $R_K = 1$ (this is true for all imaginary quadratic fields).

An Application?

We shall consider the case $K = \mathbb{Q}[i] = \mathbb{Q}(\zeta_4)$. Its ring of integers is $\mathbb{Z}[i]$, which is a PID and hence, $h_K = 1$. Now, $\{1, i\}$ forms an integral basis. A simple computation gives

$$\Delta_K = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4.$$

Finally, $r_1 = 0$ and $r_2 = 1$, whence $R_K = 1$ (this is true for all imaginary quadratic fields). Putting this into the class number formula,

$$L(1, \chi) = \frac{(2\pi)^1 \times 1 \times 1}{4 \times \sqrt{4}} = \frac{\pi}{4},$$

where χ is the unique nontrivial Dirichlet character modulo 4.

An Application?

We shall consider the case $K = \mathbb{Q}[i] = \mathbb{Q}(\zeta_4)$. Its ring of integers is $\mathbb{Z}[i]$, which is a PID and hence, $h_K = 1$. Now, $\{1, i\}$ forms an integral basis. A simple computation gives

$$\Delta_K = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4.$$

Finally, $r_1 = 0$ and $r_2 = 1$, whence $R_K = 1$ (this is true for all imaginary quadratic fields). Putting this into the class number formula,

$$L(1, \chi) = \frac{(2\pi)^1 \times 1 \times 1}{4 \times \sqrt{4}} = \frac{\pi}{4},$$

where χ is the unique nontrivial Dirichlet character modulo 4. We have successfully computed the infinite sum

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}.$$

Thank you for your attention!

The main reference for this talk is the wonderful GTM book by Robert J. Valenza and Dinakar Ramakrishnan titled

Fourier Analysis on Number Fields.

Chapter 7 of the book is the relevant chapter, which is an exposition of Tate's Thesis (1950) titled

Fourier analysis in number fields, and Hecke's zeta-functions.